(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 655 922 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.05.2006 Bulletin 2006/19

(21) Application number: **05023076.2**

(22) Date of filing: **21.10.2005**

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04L 12/28*** *(2006.01)*
G06F 1/00 *(2006.01)* ***G06K 19/00*** *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **08.11.2004 JP 2004324075**

(71) Applicant: **CANON KABUSHIKI KAISHA**
Ohta-ku, Tokyo (JP)

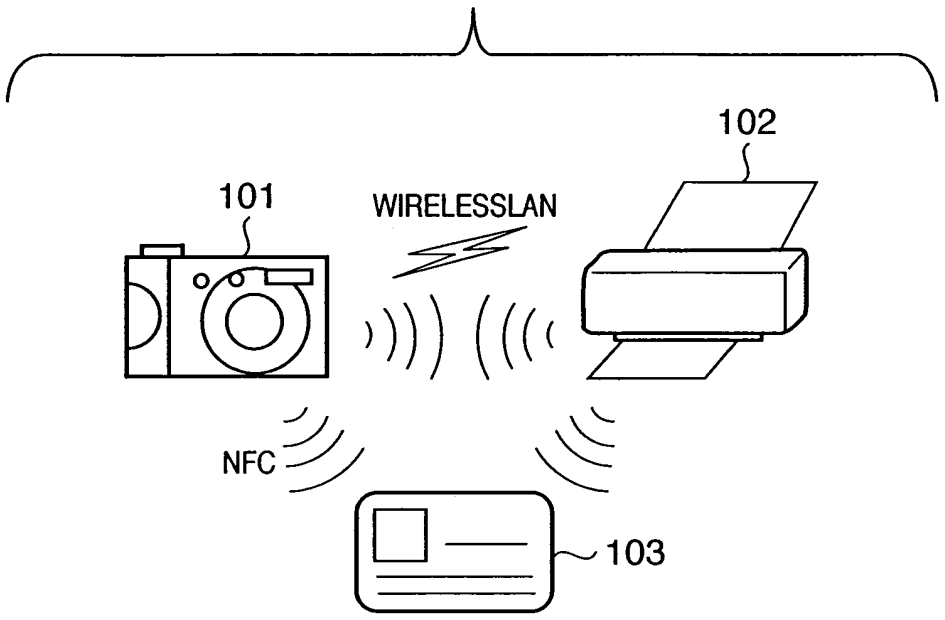
(72) Inventor: **Sakai, Tatsuhiko**
Ohta-ku
Tokyo (JP)

(74) Representative: **Weser, Wolfgang**
Weser & Kollegen,
Patentanwälte,
Radeckestrasse 43
81245 München (DE)

(54) Authentication method and system, and information processing method and apparatus

(57) When having established communication with a data processing apparatus, a first apparatus determines whether or not to generate authentication information based on identification information about the data processing apparatus. If it is determined that generation of authentication information is necessary, then the first apparatus generates authentication information and saves it in a memory. If it is determined that generation of authentication information is necessary, the first apparatus sends the generated authentication information to the data processing apparatus with which communication has been established. If it is determined that generation of authentication information is unnecessary, then the first apparatus sends authentication information saved in the memory to the data processing apparatus with which communication has been established. Thereby, authentication between data processing apparatuses is performed with the use of the authentication information sent from the first apparatus.

FIG. 1



EP 1 655 922 A1

Description

FIELD OF THE INVENTION

[0001] The present invention relates to an authentication technique for a communication system using wireless communication.

BACKGROUND OF THE INVENTION

[0002] With recent development of wireless communication techniques including WirelessLAN, it is being promoted to replace a part of a communication system using wired communication with a wireless communication system in home or office environments. For example, instead of connecting a notebook computer to a wired LAN network to perform communication by connecting a network cable with the notebook computer to connect to the network, connection may be made to a network via an access point with the use of WirelessLAN. As another example, instead of printing an image taken by a digital camera with a printer by connecting the digital camera and the printer via a USB cable or the like to transfer the image, the image may be transferred to the printer with the use of Bluetooth or WirelessLAN.

[0003] In addition to the purpose of replacing wired communication, there is great expectation for a close range wireless communication mode such as NFC (Near Field Communication). It is possible to perform communication between pieces of equipment provided with NFC only by bringing the pieces of equipment close to each other. Therefore, NFC has gotten attention as such as can provide a user with convenient means for easily utilizing various services in performing settlement processing, processing for accessing to services or the like.

[0004] From the above situation, it is anticipated that wireless communication such as WirelessLAN and NFC will further spread. That is, it is anticipated that, not only in homes and offices but also in every environment, a scene will be more often seen that various pieces of equipment provided with the above-described wireless communication mode perform communication so that a user can utilize various services.

[0005] In the case where many pieces of equipment can perform wireless communication as described above, it is essential to certainly grasp what kinds of equipment are connected to each network and perform authentication processing to avoid improper connection or connection from malicious equipment. For example, in a home environment, it must be avoided to wrongly connect to a printer of the next house when an image taken by a digital camera is printed. In an office environment, it is necessary to certainly perform authentication processing in connecting to an access point in order to prevent a malicious third person from invading an intranet.

[0006] For example, in IEEE 802.11, an authentication method utilizing a common key cryptography or an authentication method utilizing an authentication server such as RADIUS is used for such authentication processing. In Bluetooth, access control is performed by inputting a password such as a PIN code.

[0007] As described above, in an environment where wireless communication is widely and generally spread, it is necessary to prevent improper connection or invalid access by certainly performing authentication processing.

[0008] However, if consideration is given to authentication processing to be performed when portable terminals, such as a digital camera and a mobile printer provided with a wireless communication function, communicate with each other, the authentication methods described above are not necessarily suitable. For example, in general, a portable terminal does not have sufficient input means for authentication or is not provided with such input means at all. Accordingly, even if a user attempts authentication by inputting a password in such an environment, it may be very troublesome for the user to input the password, or input itself may be impossible. It is also impossible to use the method utilizing an authentication server in such an ad-hoc environment where a network is constituted only by terminals to perform communication, because there is not an authentication server on the network. Furthermore, it is also impossible for the method utilizing a common key cryptography to completely prevent access from those other than an authorized user, because security in key exchange is not specifically provided and, therefore, there is a possibility that a key may be obtained by a third person intentionally or by mistake.

[0009] In Japanese Patent Laid-Open No. 2001-189722 and in Japanese Patent Laid-Open No. 2003-174468, there is proposed an authentication system utilizing a card.

[0010] However, in such a system, it is possible for a third person to acquire information for authentication from each equipment by using an apparatus provided with a data reading/writing function equivalent to that of the card. Therefore, the system also cannot enable satisfactory security to be obtained.

SUMMARY OF THE INVENTION

[0011] The present invention has been made in consideration of the above problems, and its object is to make it possible to easily and certainly perform authentication processing without annoying a user with a troublesome work even in an environment where access to an authentication server is impossible due to insufficient user interface of a portable terminal.

[0012] In order to achieve the above object, according to one aspect of the present invention, there is provided an authentication method for performing authentication between data processing apparatuses, the method comprising: a determination step of, when communication is established with a data processing apparatus, determin-

ing whether or not generation of authentication information is necessary based on identification information about the data processing apparatus, in a first apparatus; a generation step of, if it is determined by the determination step that generation of authentication information is necessary, generating authentication information and saving the authentication information in a memory, in the first apparatus; a first sending step of, if it is determined by the determination step that generation of authentication information is necessary, sending the authentication information generated by the generation step to the data processing apparatus with which communication has been established, in the first apparatus; a second sending step of, if it is determined by the determination step that generation of authentication information is unnecessary, sending authentication information saved in the memory to the data processing apparatus with which communication has been established, in the first apparatus; and an authentication step of performing authentication between the data processing apparatuses with the use of the authentication information sent by the first sending step or the second sending step.

[0013] Other features and advantageous of the present invention will be apparent from the following description taken in conjunction with the accompanying drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and , together with the description, serve to explain the principles of the invention.

FIG. 1 shows an example of configuration of an authentication system according to this embodiment;
FIG. 2 is a block diagram showing functional configuration of an image capturing apparatus in the authentication system of this embodiment;
FIG. 3 is a block diagram showing functional configuration of a printer applicable to the authentication system of this embodiment;
FIG. 4 is a block diagram showing functional configuration of an authentication card applicable to the authentication system of this embodiment;
FIG. 5 is a sequence diagram showing a procedure for authentication processing in this embodiment;
FIG. 6 is a flowchart showing a procedure for authentication information sending processing to be performed in the authentication card of this embodiment;
FIG. 7 is a flowchart showing a procedure for authentication processing in a printer of this embodiment, which is an apparatus to perform authentication;
FIG. 8 is a flowchart illustrating the operation of the printer in the authentication processing;
FIG. 9 is a flowchart illustrating the operation of the image capturing apparatus in the authentication processing; and
FIG. 10 is a flowchart illustrating the operation of the authentication card in the authentication processing.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0015] Preferred embodiments of the present invention will now be described in detail in accordance with the accompanying drawings.

[First Embodiment]

[0016] FIG. 1 shows the outline of configuration of a wireless system to which authentication processing according to a first embodiment is applicable. As shown in FIG. 1, the authentication processing of the first embodiment realizes authentication between an image capturing apparatus 101 and a printer 102 by causing an authentication card 103 to intervene therebetween. That is, in the wireless communication system of the first embodiment, the image capturing apparatus 101, the printer 102 and the authentication card 103 perform authentication processing utilizing close range wireless communication by means of NFC. Then, if the authentication processing succeeds and access is permitted, content data is communicated from the image capturing apparatus 101 to the printer 102 by means of WirelessLAN.

[0017] The configuration of the image capturing apparatus 101 in this embodiment will be described with the use of the functional block diagram shown in FIG. 2. The image capturing apparatus 101 is provided at least with a WirelessLAN communication section 201, an NFC reader/writer communication section 202, an authentication processing section 203, a storage section 204 and an image capturing processing section 205. The WirelessLAN communication section 201 has a function of performing wireless communication with neighbor terminals utilizing the WirelessLAN communication mode. The NFC reader/writer communication section 202 has a function of forming an RF field with an NFC tag or another NFC reader/writer communication section within the communication distance utilizing the NFC communication mode to send and receive data. The authentication processing section 203 has a function of accessing another apparatus (in this example, the printer 102) and performing authentication processing to perform WirelessLAN communication. The storage section 204 has a function of storing authentication information acquired from the outside (in this example, the authentication card 103). The image capturing processing section 205 has a function of performing processing related to image capturing, which is the main function of the image capturing apparatus 101.

[0018] Next, the configuration of the printer 102 in this

embodiment will be described with the use of the functional block diagram shown in FIG. 3. The printer 102 is provided at least with a WirelessLAN communication section 301, an NFC reader/writer communication section 302, an authentication processing section 303, a storage section 304, a print processing section 305 and a timer section 306. The WirelessLAN communication section 301 has a function of performing wireless communication with neighbor terminals utilizing the WirelessLAN communication mode. The NFC reader/writer communication section 302 has a function of forming an RF field with an NFC tag or another NFC reader/writer communication section within the communication distance utilizing the NFC communication mode to send and receive data. The authentication processing section 303 has a function of performing authentication processing for a terminal requesting permission of WirelessLAN communication access. The storage section 304 has a function of storing identification information and authentication information to be acquired from the outside (in this example, the authentication card 103). The print processing section 305 has a function of performing processing related to printing, which is the main function of the printer 102. The timer section 306 has a function of monitoring the time limit of validity of authentication information stored in the storage section 304.

[0019] Next, the configuration of the authentication card 103 according to this embodiment will be described with the use of the functional block diagram shown in FIG. 4. The authentication card 103 is provided at least with an NFC tag communication section 401, an authentication information management section 402, an authentication information generation section 403 and a storage section 404. The NFC tag communication section 401 is activated by being supplied with power from an RF field formed between the NFC tag communication section 401 and an NFC reader/writer section within the communication distance, through electromagnetic induction. Then, the NFC tag communication section 401 performs communication by returning a response to a request from the NFC reader/writer section. The authentication information management section 402 has a function of performing authentication information sending processing in response to an authentication information request message. The authentication information generation section 403 generates authentication information. In this embodiment, the authentication information generation section 403 has a function of generating a random character string with several digits as the authentication information every time it is activated. Though a random character string with several digits is used as the authentication information in this embodiment, the data length and the data format are not limited thereto. That is, any data can be used as the authentication information if it can be communicated between terminals, stored in the storage section of each terminal and compared. The storage section 404 has a function of storing the authentication information generated by the authentication information generation section 403.

[0020] The image capturing apparatus 101, the printer 102 and the authentication card 103 have hardware configuration for realizing the functional configuration shown in FIGS. 2 to 4, respectively. Such configurations, however, are apparent to those skilled in the art, and therefore, illustration by figures is omitted here. As an example of configuration of the WirelessLAN communication section, there is configuration for performing WirelessLAN communication in conformity with the IEEE 802.11 standard or the like. For configuration for performing NFC (202, 302 and 401), RFID (Radio Frequency Identification) can be used. Description will be made below on authentication processing to be performed when WirelessLAN communication is performed between the image capturing apparatus 101 and the printer 102.

[0021] Next, description will be made on the flow of processing by the authentication method according to the first embodiment with the use of FIG. 5 and FIGS. 8 to 10. FIG. 5 shows connection and information flow among the image capturing apparatus 101 as an apparatus which requests authentication, the printer 102 as an apparatus which confirms authentication and the authentication card 103 as an apparatus which provides authentication information. FIGS. 8, 9 and 10 are flowcharts illustrating the authentication processing operations of the printer 102, the image capturing apparatus 101 and the authentication card 103, respectively.

[0022] First, the printer 102 and the authentication card 103 perform processing for exchanging identification information and store identification information about the counterpart in their storage sections (304 and 404), respectively (step S501). This is called "pairing", which is performed to prevent authentication card spoofing in the authentication method described below. As the identification information, unique information which never overlaps with ID's of other equipment is used, such as a UUID (Universally Unique IDentifier). The following are possible methods for pairing (methods for causing the printer 102 and the authentication card 103 to store the identification information about the counterpart):

(1) A method in which an authorized user inputs the authentication information about the authentication card 103 from the operation section of the printer 102 for storage;

(2) A method in which the authentication information about the authentication card 103 is inputted into the printer 102 for storage by operating a computer connected to the printer 102 via a cable;

(3) A method in which the pieces of identification information are exchanged by operation by an authorized user, with the use of NFC communication; and

(4) A method in which the identification information about the counterpart is written in the storage section before factory shipment.

[0023] Next, the authentication card 103 is brought close to the printer 102 until it is within the distance enabling NFC communication with the printer 102. Then, an RF field is formed between the authentication card 103 and the printer 102, and NFC communication is established and started (step S502). When NFC communication is started with the authentication card 103, the printer 102 sends a message requesting the identification information of the authentication card 103 to the authentication card 103 (step S503). In response to this request, the authentication card 103 sends its identification information to the printer 102 (step S504).

[0024] The printer 102 compares the acquired identification information of the authentication card 103 and the identification information stored in the storage section 304 to check whether the authentication card performing the NFC communication is the terminal which has performed the identification exchange processing (pairing) at step S501. If the pieces of identification information correspond to each other as a result of the comparison, then the printer 102 sends an authentication information request message including its identification information to the authentication card 103 (step S505). On the other hand, if the pieces of identification information do not correspond to each other, then the authentication processing is terminated. In this case, for example, a message representing the above status may be sent from the printer 102 to the authentication card 103, or the processing may be immediately terminated. If the printer 102 immediately terminates the processing, nothing is notified to the authentication card 103. However, the authentication card 103 can detect the termination of the processing from the fact that a predetermined time has elapsed without receiving a response since it sent its identification information response.

[0025] Having received the authentication information request message from the printer 102, the authentication card 103 performs authentication information sending processing to be described later to return a suitable authentication information response message to the printer 102 (step S506). That is, the authentication card 103 compares the identification information about the printer 102 included in the authentication information request message and the identification information stored in the storage section 404 to check whether the printer 102 is the terminal which has performed the identification information exchange processing at step S501. If the pieces of identification information correspond to each other as a result of the comparison, then the authentication information request is permitted, and the authentication card 103 generates authentication information, stores the authentication information in an authentication information response message and sends the message to the printer 102. If the authentication information is included in the received response message, the printer 102 stores the authentication information in the storage section 304. Here, the printer 102 activates the timer section 306 for saving authentication information, and discards the stored authentication information when the time limit of the timer comes. If the authentication information response message is an error, then the printer terminates the authentication processing.

[0026] Through the above-described processing from steps S501 to S506, the authentication information is sent from the authentication card 103 to the printer 102. Next, by the user bringing the authentication card 103 close to the image capturing apparatus 101 until it is within the distance enabling NFC communication, the authentication card 103 forms an RF field with the image capturing apparatus 101, and establishes and starts NFC communication (step S507). When NFC communication is started, the image capturing apparatus 101 sends an authentication information request message including its identification information to the authentication card 103 (step S508).

[0027] Receiving the authentication information request message from the image capturing apparatus 101, the authentication card 103 performs authentication information sending processing to be described later to return a suitable authentication information response message to the image capturing apparatus 101 (step S509). Here, the authentication card 103 compares the identification information about the image capturing apparatus 101 included in the authentication information request message and the identification information stored in the storage section 404. Then, according to the result of the comparison, the authentication card 103 includes the same authentication information as has been sent at step S506 in an authentication information response message and sends the message to the image capturing apparatus 101. If the authentication information is included in the received response message, the image capturing apparatus 101 stores the authentication information in the storage section 204. If the authentication information response message is an error, then the image capturing apparatus 101 terminates the authentication processing.

[0028] When sending of the authentication information to the printer 102 and the image capturing apparatus 101 is normally completed through the processing from steps S501 to S509, the common authentication information has been stored in the respective storage sections (204 and 304) of the image capturing apparatus 101 and the printer 102. After that, when the user brings the image capturing apparatus 101 close to the printer 102 until it is within the distance enabling NFC communication, an RF field is formed between the image capturing apparatus 101 and the printer 102, and NFC communication is established and started (step S510).

[0029] When communication is started at step S510, the authentication processing section 203 of the image capturing apparatus 101 reads the authentication information stored in the storage section 204 at step S509, and sends an authentication request message in which the read authentication information is stored to the printer 102 (step S511). Receiving the authentication request

message from the image capturing apparatus 101, the authentication processing section 303 of the printer 102 performs authentication processing to be described later to determine whether or not access from the image capturing apparatus 101 should be permitted, and sends a suitable authentication response message to the image capturing apparatus 101 (step S512). When the authentication succeeds, the image capturing apparatus 101 and the printer 102 exchange setting information required for WirelessLAN communication, such as network identifiers (ESSID), encryption keys being communicated and information about the frequency channel to be used, through the NFC communication (step S513). Then, the image capturing apparatus 101 and the printer 102 utilize the setting information exchanged at step S513 to start WirelessLAN communication (step S514). On the other hand, if authentication fails, the authentication processing is terminated.

[0030] The image capturing apparatus 101 and the printer 102 perform the authentication processing in accordance with the above-described procedure. The operations of the printer 102, the image capturing apparatus 101 and the authentication card 103 in the above authentication processing will be described below with the use of the flowcharts in FIGS. 8 to 10, respectively.

[0031] In the printer 102, when an RF field is formed, the process proceeds from step S801 to step S802, where it is determined whether or not the connection destination is the authentication card 103. If the connection destination is the authentication card 103, then the process proceeds to step S803, where identification information is requested (S503). The identification information is received from the authentication card 103. If the identification information corresponds to registered identification information, then the process proceeds from step S804 to step S805, and authentication information is requested of the authentication card 103 (S504 and S505). Here, if the identification information cannot be received within a predetermined time, or if the received identification information does not correspond to the registered identification information, then the process proceeds to step S808. At step S808, corresponding error processing (for example, notification is made to notify that the pieces of identification information do not correspond to each other or the identification information has not been received) is performed, and the present processing is terminated.

[0032] If authentication information in response to the authentication information request is received, then the process proceeds from step S806 to step S807, and the authentication information is saved in the storage section 304 (S506). In the case where the authentication information cannot be received, such as the case where the authentication information cannot be received in a predetermined time or the case where an error message is received, the process proceeds from step S806 to step S808, where corresponding error processing (for example, notification of the content of the error) is performed, and the present processing is terminated.

[0033] If the connection destination is not an authentication card, then it is determined that the connection destination is an apparatus which requests authentication (in this example, the image capturing apparatus), and the process proceeds from step S801 to step S810 to wait for receiving an authentication request. When an authentication request is received (S510 and S511), authentication processing is performed at step S811 (to be described later with reference to FIG. 7) to determine whether or not access should be permitted. If access is permitted, then the process proceeds from step S812 to step S813, where permission of access is notified to the connection destination (S512), and the setting information required for WirelessLAN communication, which is stored in the storage section 304, is notified (S513). When the notification of the setting information for WirelessLAN ends, setting for the WirelessLAN communication section 201 is made based on the notified setting information, and the process proceeds to step S814, where WirelessLAN communication is started with the connection destination (S513 and S514). On the other hand, if access is refused, then the process proceeds from step S812 to step S815, where notification to that effect is made to the connection destination (S512), a message to that effect is displayed on the operation panel of the printer 102, and then the present processing is terminated.

[0034] Meanwhile, in the image capturing apparatus 101, when an RF field is formed, the process proceeds from step S901 to step S902, where it is determined whether or not the connection destination is the authentication card 103. If the connection destination is the authentication card 103, then authentication information is requested at step S903 (S507 and S508). If the authentication information is received, then the process proceeds from step S904 to step S905, the authentication information is saved in the storage section 204, and the processing is terminated (S509). If the authentication information cannot be received in a predetermined time, or if an error message is received, then the process proceeds from step S904 to step S906, where corresponding error processing (for example, notification of the content of the error) is performed, and the present processing is terminated.

[0035] If the connection destination is not the authentication card 103, then the process proceeds from step S902 to step S910. In this case, it is determined that the connection destination is an apparatus which performs authentication confirmation, and authentication is requested with the use of the authentication information saved in the storage section 204 (S510 and S511). Then, an authentication response is received from the connection destination, and the process proceeds from step S911 to step S912 if the response indicates permission of access. At step S912, the setting information required for WirelessLAN communication, which has been sent from the printer 102, is received and stored in the storage

section 304, and setting is made for the WirelessLAN communication section 301 based on the stored setting information. When the setting has been made, the process proceeds to step S913, where LAN communication is started with the connection destination (S512 to S514). If an authentication response to the authentication request cannot be obtained, or if refusal of access is received as an authentication response, then the process proceeds from step S911 to step S914, where error processing corresponding thereto is performed (for example, the error is displayed on the display panel provided for the image capturing apparatus 101).

[0036] Meanwhile, in the authentication card 103, when an RF field is formed, the process proceeds from step S1001 to step S1002 and subsequent steps (S502 and S507). When an identification information request is received from a connection destination, the process proceeds from step S1002 to step S1003, where the identification information stored in the storage section 404 of the authentication card 103 is sent (S503 and S504). When an authentication information request is received, the process proceeds from step S1004 to step S1005, where authentication information sending processing to be described later is performed to send authentication information to the connection destination (S505, S506, S508 and S509).

[0037] Next, description will be made on the authentication information sending processing (step S1005 in FIG. 10) at the above-described steps S506 and S509 to be performed in the authentication card 103, with the use of the flowchart in FIG. 6.

[0038] First, at step S601, it is determined whether or not the identification information included in the authentication information request message corresponds to the identification information stored in the storage section 404. If the pieces of identification information correspond to each other, the process proceeds to step S602. Otherwise, the process proceeds to step S604. Here, if the identification information included in the authentication information request message corresponds to the identification information stored in the storage section 404, then it is determined that the authentication information request message has been sent from an apparatus which performs authentication (in this example, the printer 102). In this case, at step S602 and subsequent steps, new authentication information is generated and returned to the requesting side. On the other hand, if the identification information included in the authentication information request message does not correspond to the identification information stored in the storage section 404, then it is determined that the authentication information request message has been sent from an apparatus which requests authentication (in this example, the image capturing apparatus 101). In this case, at step S604 and subsequent steps, authentication information which has already been generated and saved is returned to the requesting side. In other words, in the above-described processing, it is determined whether or not to generate authentication information, based on identification information included in an authentication information request, and authentication information is generated at step S602 if it is determined that the information should be generated. Accordingly, as for how identification information should be used to determine whether or not to generate authentication information, it is possible to make various changes.

[0039] At step S602, authentication information is generated by the authentication information generation section 403, and at step S603, the generated authentication information is stored in the storage section 404. At step S604, the authentication information stored in the storage section 404 is read, and at step S605, a response message in which the read authentication information is included is created and sent to the communication counterpart terminal.

[0040] According to the above-described processing, if an authentication information request message is received from the printer 102 with which identification information has been exchanged (S505), new authentication information is generated by the authentication information generation section 403. Then, this authentication information is notified to the printer 102 (the authentication information response at S506) and stored in the storage section 404. If an authentication information request message is received from the image capturing apparatus 101 with which identification information has not been exchanged (S508), the authentication information saved in the storage section 404 is simply read and notified to the image capturing apparatus 101 (the authentication information response at S509).

[0041] The printer 102 and the image capturing apparatus 101 which have received a response message by the authentication information response at the above-described steps S506 and S509 save authentication information included in the response message in the storage sections (304 and 204), respectively.

[0042] Next, description will be made on the authentication processing (S811 in FIG. 8) to be performed by the printer 102 as an apparatus which performs authentication, for the authentication response at step S512, with the use of FIG. 7. The processing in FIG. 7 shows processing to be performed by receiving an authentication request message from the image capturing apparatus 101 as an apparatus which requests authentication.

[0043] When an authentication request message is received, it is determined first at step S701 whether or not authentication information is stored in the storage section 304. If the authentication information is stored in the storage section 304, then the process proceeds to step S702. On the other hand, if the authentication information is not stored in the storage section 304, then the process proceeds to step S704. The following are the reasons why the authentication information is not stored in the storage section 304:

(1) The printer 102 has not acquired the authentica-

tion information from the authentication card 103;
(2) The authentication information has been already deleted as used information at step S705 to be described later;
(3) The authentication information has been deleted because the time limit of the timer activated at step S506 came; and the like.

[0044] At step S702, authentication information stored in the authentication request message and the authentication information stored in the storage section 304 are compared to determine whether or not the pieces of authentication information correspond to each other. If both pieces correspond to each other, then the process proceeds to step S703 on the assumption that the authentication has succeeded. Otherwise, the process proceeds to step S704. At step S703, a response message which includes information indicating permission of access is sent to the terminal which sent the authentication request message. Then, the process proceeds to step S705, where the authentication information stored in the storage section 304 is deleted, and the processing is terminated.

[0045] If the authentication information is not stored in the storage section 304, or if the authentication information stored in the storage section 304 and the authentication information included in the authentication request message do not correspond to each other, then it is determined that authentication has failed. Accordingly, at step S704, information indicating refusal of access and a response message which includes the reason of the refusal of access, such as "no authentication information stored on the printer side" and "authentication information not corresponding to each other" is sent to the communication counterpart terminal, and the processing is terminated. In this case, a message to the effect that authentication has failed may be displayed on the operation panel of the printer 102.

[0046] When having formed an RF field with the printer 102, the image capturing apparatus 101 sends an authentication request message which includes the authentication information saved in its storage section 204 to the printer 102 and waits for an authentication result (permission of access or failure of authentication). If access is permitted, then setting information for WirelessLAN is exchanged with the printer 102, and connection for WirelessLAN communication is established. If failure of authentication is notified, a message to that effect may be displayed.

[0047] Through the above-described processing, the authentication processing between the image capturing apparatus 101 and the printer 102 is performed. Next, description will be made on how authentication fails if the user fails to perform operation in accordance with the procedure in FIG. 5.

[0048] For example, there may be a case where the user brings the authentication card 103 which has already exchanged identification information at step S501 close to the image capturing apparatus 101 before performing the authentication information sending processing with the printer 102, and performs the authentication information sending processing with the image capturing apparatus 101. In this case, the authentication information stored in the storage section 404 of the authentication card 103 is sent to the image capturing apparatus 101 in accordance with the above-described procedure in FIG. 6. However, this authentication information has been used for the previous authentication processing. Therefore, it is conceivable that the printer 102 discarded the authentication information at step S705 when the previous authentication processing succeeded or discarded it on the assumption that the time limit came based on the processing of the timer section 306 of the printer 102. Accordingly, in this case, when authentication is requested by bringing the image capturing apparatus 101 close to the printer 102, failure of authentication is notified at step S704 because authentication information has not been stored at step S701. In this case, an access refusal message may be sent which includes "no authentication information" as the reason of refusal. The image capturing apparatus 101, for which access has been refused, notifies the user that an error has occurred by displaying the reason of refusal on the operation screen or the like and that there is no authentication information in the printer 102. From this notification, the user can recognize that he should retry the authentication processing from step S502.

[0049] As another example, there may be a case where the user requests authentication by bringing the image capturing apparatus 101 close to the printer 102 without bringing the authentication card 103 close to the image capturing apparatus 101, after the authentication card 103 performs the authentication information sending processing with the printer 102 as the target. In this case, the authentication information generated at step S602 and sent at step S506 is not stored in the storage section 204 of the image capturing apparatus 101. That is, since correct authentication information is not stored, the pieces of authentication information do not correspond to each other at step S702, and failure of authentication is notified at step S704. In this case, an access refusal message may be sent which includes "authentication information not corresponding to each other" as the reason of refusal. The image capturing apparatus 101, for which access has been refused, notifies the user that an error has occurred by displaying the reason of refusal on the operation screen or the like. From this notification, the user can recognize that correct authentication information is not stored in the image capturing apparatus 101 and determine that he can retry the authentication processing from step S507.

[0050] In the above description, as an example of the exchange of setting information at step S513 in FIG. 5, setting information for WirelessLAN communication is sent from the printer 102 to the image capturing apparatus 101 so that the WirelessLAN setting for the printer

102 may be also made for the image capturing apparatus 101. However, the exchange is not limited thereto. The image capturing apparatus 101 may send setting information for WirelessLAN stored in the storage section 204 to the printer 102 so that the WirelessLAN setting for the image capturing apparatus 101 may be made for the printer 102.

[0051] As described above, according to the above-described embodiment, it is possible for a user to easily and certainly perform authentication processing only by simply bringing an authentication card close to an apparatus which performs authentication and an apparatus which requests authentication without performing troublesome work such as input of a password. Furthermore, according to the authentication method of this embodiment, it is possible to perform authentication processing without performing a procedure for connecting to an authentication server via an access point. Accordingly, it is possible to easily and certainly perform authentication processing even in an ad hoc communication environment where connection to infrastructure such as a base station and an access point is impossible. Furthermore, according to the authentication method of the above-described embodiment, it is possible to easily give access permission even to equipment that has not performed registration processing and the like while preventing spoofing or invalid access.

[0052] In the present invention, there is also included a case where software programs for realizing the functions of the embodiment described above (in the embodiment, programs corresponding to the flowcharts shown in the figures) are supplied to a system or an apparatus directly or remotely, and the computer of the system or the apparatus reads and executes the supplied program codes to achieve the functions of the embodiment described above.

[0053] Accordingly, the program codes themselves, which are to be installed in the computer to realize the functions and processing of the present invention by means of the computer, also realize the present invention. That is, the present invention includes the computer programs themselves which are for realizing the functions and processing of the present invention.

[0054] In this case, the computer programs may be in the form of object codes, programs to be executed by an interpreter, script data to be supplied to the OS or the like only if they have functions as a program.

[0055] As a recording medium for supplying the programs, there are, for example, a floppy® disk, hard disk, optical disk, magneto-optical disk, MO, CD-ROM, CD-R, CD-RW, magnetic tape, non-volatile memory card, ROM, DVD (DVD-ROM, DVD-R) and the like.

[0056] In addition, as another method for supplying the programs, it is also possible to connect to an Internet web page with the use of a browser of a client computer and download the computer programs of the present invention themselves or a compressed file including an automatic installation function from the web page to a recording medium such as a hard disk. Furthermore, it is also possible to divide the program codes of the programs of the present invention into multiple files so that each file may be downloaded from a different web page. That is, a WWW server which enables multiple users to download program files for realizing the functions and processing of the present invention with a computer is also included in the present invention.

[0057] Furthermore, it is also possible to encrypt the programs of the present invention, store them in a storage medium such as a CD-ROM and distribute the CD-ROM to users in order to enable a user who satisfies predetermined conditions to download key information for decryption from a web page via the Internet, use the key information to execute the encrypted programs, install them on a computer and realize them.

[0058] Furthermore, in addition to the case where the functions of the embodiment described above are realized by a computer executing the read programs, the functions of the embodiment described above can be realized by an OS or the like, which is operating on the computer, performing a part or all of the actual processing based on instructions of the programs.

[0059] Furthermore, the functions of the embodiment described above can be realized by the CPU provided for a feature expansion board inserted in a computer or a feature expansion unit connected to the computer performing a part or all of the actual processing based on instructions of the programs, which have been read from a recording medium and written in the memory provided for the feature expansion board or the feature expansion unit.

[0060] According to the present invention, it is possible to easily and certainly perform authentication processing without annoying a user with troublesome work even in an environment where access to an authentication server is impossible due to insufficient user interface of an apparatus.

[0061] As many apparently widely different embodiments of the present invention can be made without departing from the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

Claims

1. An authentication method for performing authentication between data processing apparatuses, the method **characterized by** comprising:

   a determination step of, when communication is established with a data processing apparatus, determining whether or not generation of authentication information is necessary based on identification information about the data processing apparatus, in a first apparatus;

a generation step of, if it is determined by the determination step that generation of authentication information is necessary, generating authentication information and saving the authentication information in a memory, in the first apparatus;

a first sending step of, if it is determined by the determination step that generation of authentication information is necessary, sending the authentication information generated by the generation step to the data processing apparatus with which communication has been established, in the first apparatus;

a second sending step of, if it is determined by the determination step that generation of authentication information is unnecessary, sending authentication information saved in the memory to the data processing apparatus with which communication has been established, in the first apparatus; and

an authentication step of performing authentication between the data processing apparatuses with the use of the authentication information sent by the first sending step or the second sending step.

2. The method according to claim 1, further comprising:

an establishment step of, if authentication is given by the authentication step, establishing communication by a protocol different from the protocol for the communication used at the authentication step between the data processing apparatuses.

3. The method according to claim 1, further comprising:

an invalidation step of invalidating the authentication information after a predetermined period, in the data processing apparatus which has received the authentication information sent by the first or second sending step.

4. The method according to claim 1, further comprising:

an invalidation step of invalidating the authentication information when authentication is given at the authentication step, in the data processing apparatus which has received the authentication information sent by the first or second sending step.

5. The method according to claim 1, wherein
the determination step determines that generation of authentication information is necessary if identification information registered with the first apparatus in advance corresponds to identification information about the data processing apparatus with which communication has been established.

6. The method according to claim 1, wherein
the communication established at the determination step is near field communication.

7. The method according to claim 1, wherein
the communication established between the data processing apparatuses at the authentication step is near field communication.

8. An information processing method for providing authentication information to an external apparatus, the method comprising
an establishment step of establishing communication with the external apparatus,
wherein the method is **characterized by** comprising:

a determination step of acquiring identification information about the external apparatus via the communication established at the establishment step and determining whether or not to generate authentication information based on the acquired identification information;

a generation step of, if it is determined at the determination step to generate authentication information, generating authentication information and saving the authentication information in a memory; and

a sending step of sending the authentication information generated at the generation step to the external apparatus via the established communication if it is determined at the determination step to generate authentication information, and sending identification information saved in the memory to the external apparatus via the established communication if it is determined at the determination step that generation of authentication information is unnecessary.

9. The method according to claim 8, wherein
the communication established at the establishment step is near field communication.

10. An information processing method for performing authentication in communicating with an external apparatus, the method **characterized by** comprising:

a first acquisition step of establishing communication with a first external apparatus and, if it is determined that the first external apparatus is a particular apparatus, acquiring authentication information from the first external apparatus and saving the authentication information in a memory;

a second acquisition step of establishing communication with a second external apparatus

and acquiring authentication information from the second external apparatus; and
an authentication step of performing authentication with the use of the authentication information saved in the memory and the authentication information acquired at the second acquisition step.

11. The method according to claim 10, further comprising:

an establishment step of, if authentication is given by the authentication step, establishing communication by a protocol different from the protocol for the communication used at the first acquisition step and the authentication step with the second external apparatus.

12. The method according to claim 10, wherein
the communication established at the first acquisition step and the second acquisition step is near field communication.

13. The method according to claim 10, further comprising:

an invalidation step of invalidating the authentication information saved in the memory if authentication is given by the authentication step.

14. The method according to claim 10, further comprising:

an invalidation step of invalidating the authentication information saved in the memory after a predetermined period.

15. A system having a first apparatus and a plurality of data processing apparatuses, wherein the system is **characterized in that**
said first apparatus comprises:

determination means for, when communication is established with a data processing apparatus, determining whether or not generation of authentication information is necessary based on identification information about the data processing apparatus;
generation means for, if it is determined by said determination means that generation of authentication information is necessary, generating authentication information and saving the authentication information in a memory;
first sending means for, if it is determined by said determination means that generation of authentication information is necessary, sending the authentication information generated by said generation means to the data processing apparatus with which communication has been established; and
second sending means for, if it is determined by said determination means that generation of authentication information is unnecessary, sending authentication information saved in the memory to the data processing apparatus with which communication has been established; and
each of said plurality of data processing apparatuses comprising authentication means for performing authentication between said data processing apparatuses with the use of the authentication information sent by said first sending means or said second sending means.

16. An information processing apparatus which provides authentication information for an external apparatus, the information processing apparatus comprising
establishment means for establishing communication with the external apparatus,
wherein said apparatus is **characterized by** comprising:

determination means for acquiring identification information about the external apparatus via the communication established by said establishment means and determining whether or not to generate authentication information based on the acquired identification information;
generation means for, if it is determined by said determination means to generate authentication information, generating authentication information and saving the authentication information in a memory; and
sending means for sending the authentication information generated by said generation means to the external apparatus via the established communication if it is determined by said determination means to generate authentication information, and sending identification information saved in the memory to the external apparatus via the established communication if it is determined by said determination means that generation of authentication information is unnecessary.

17. An information processing apparatus which performs authentication in communicating with an external apparatus, the information processing apparatus **characterized by** comprising:

first acquisition means for establishing communication with a first external apparatus and, if it is determined that the first external apparatus is a particular apparatus, acquiring authentication information from the first external apparatus and saving the authentication information in a mem-

ory;

second acquisition means for establishing communication with a second external apparatus and acquiring authentication information from the second external apparatus; and

authentication means for performing authentication with the use of the authentication information saved in the memory and the authentication information acquired by said second acquisition means.

FIG. 1

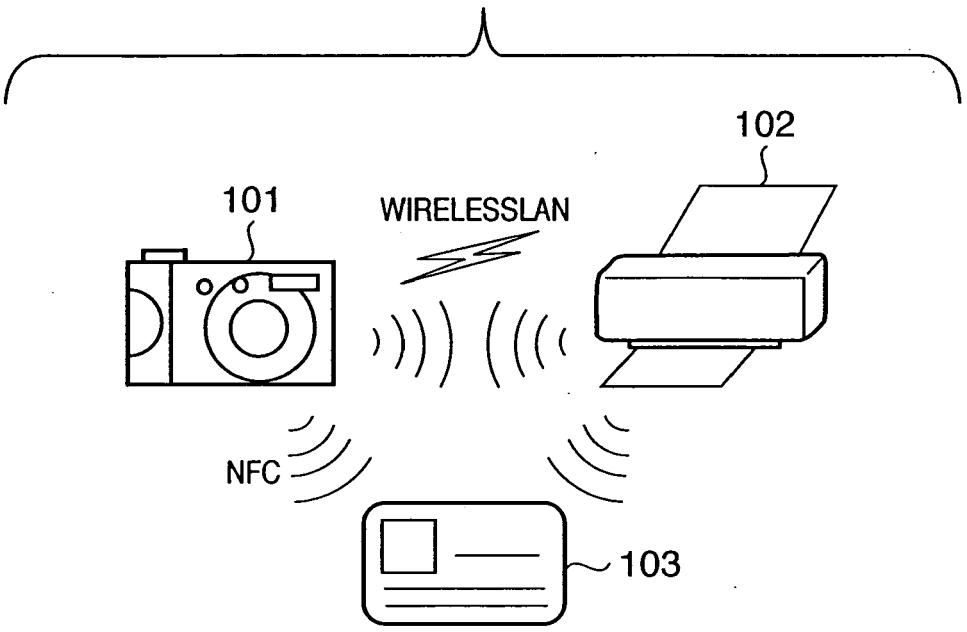


FIG. 2

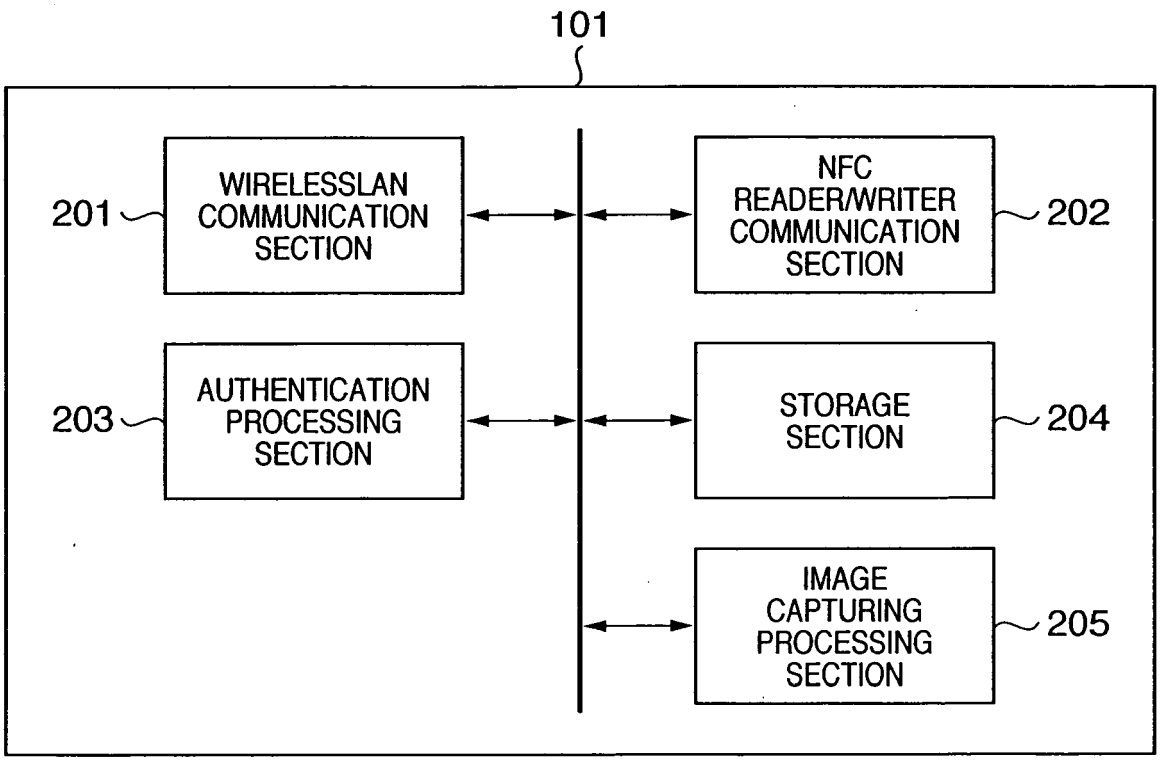

101
201
WIRELESSLAN COMMUNICATION SECTION
NFC READER/WRITER COMMUNICATION SECTION
202
203
AUTHENTICATION PROCESSING SECTION
STORAGE SECTION
204
IMAGE CAPTURING PROCESSING SECTION
205

FIG. 3

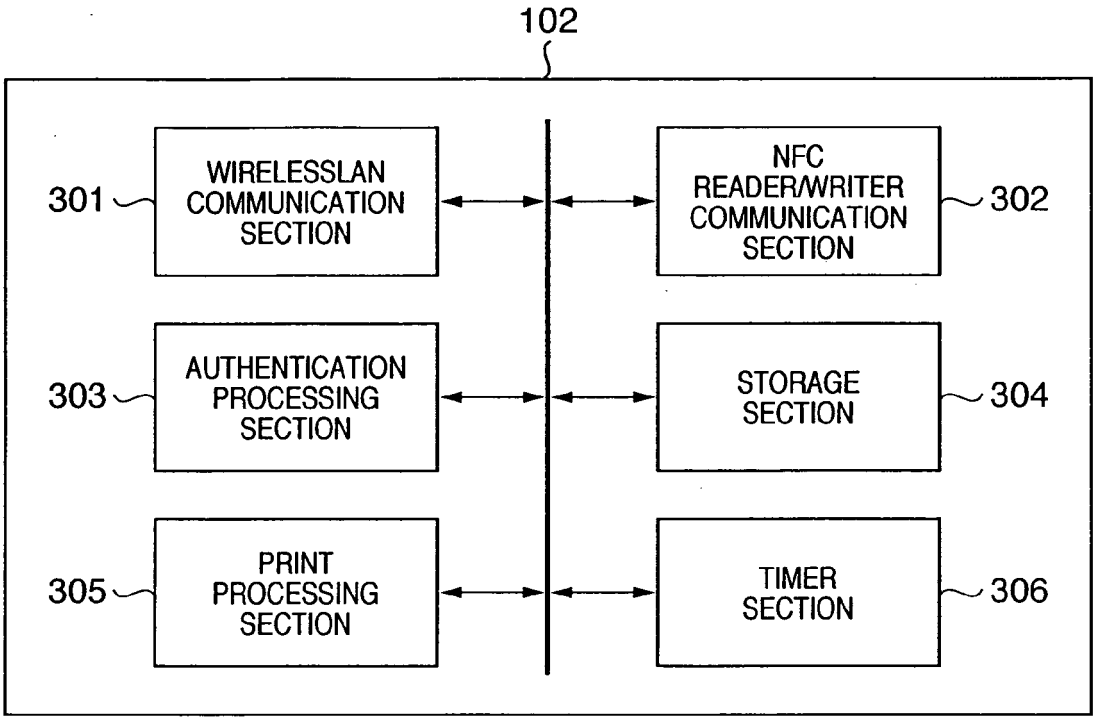

102
301
WIRELESSLAN COMMUNICATION SECTION
NFC READER/WRITER COMMUNICATION SECTION
302
303
AUTHENTICATION PROCESSING SECTION
STORAGE SECTION
304
305
PRINT PROCESSING SECTION
TIMER SECTION
306

FIG. 4

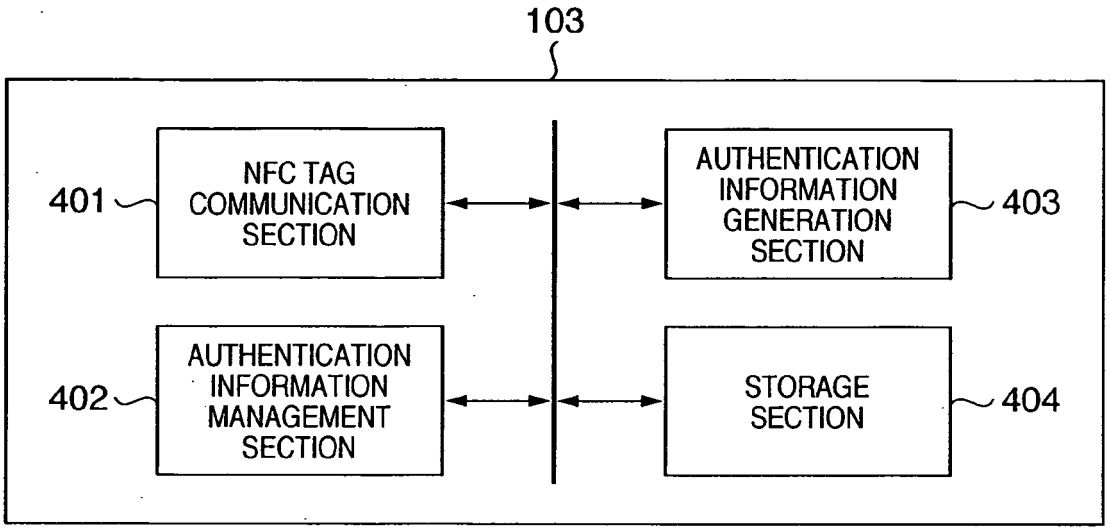

103
401
NFC TAG COMMUNICATION SECTION
AUTHENTICATION INFORMATION GENERATION SECTION
403
402
AUTHENTICATION INFORMATION MANAGEMENT SECTION
STORAGE SECTION
404

FIG. 5

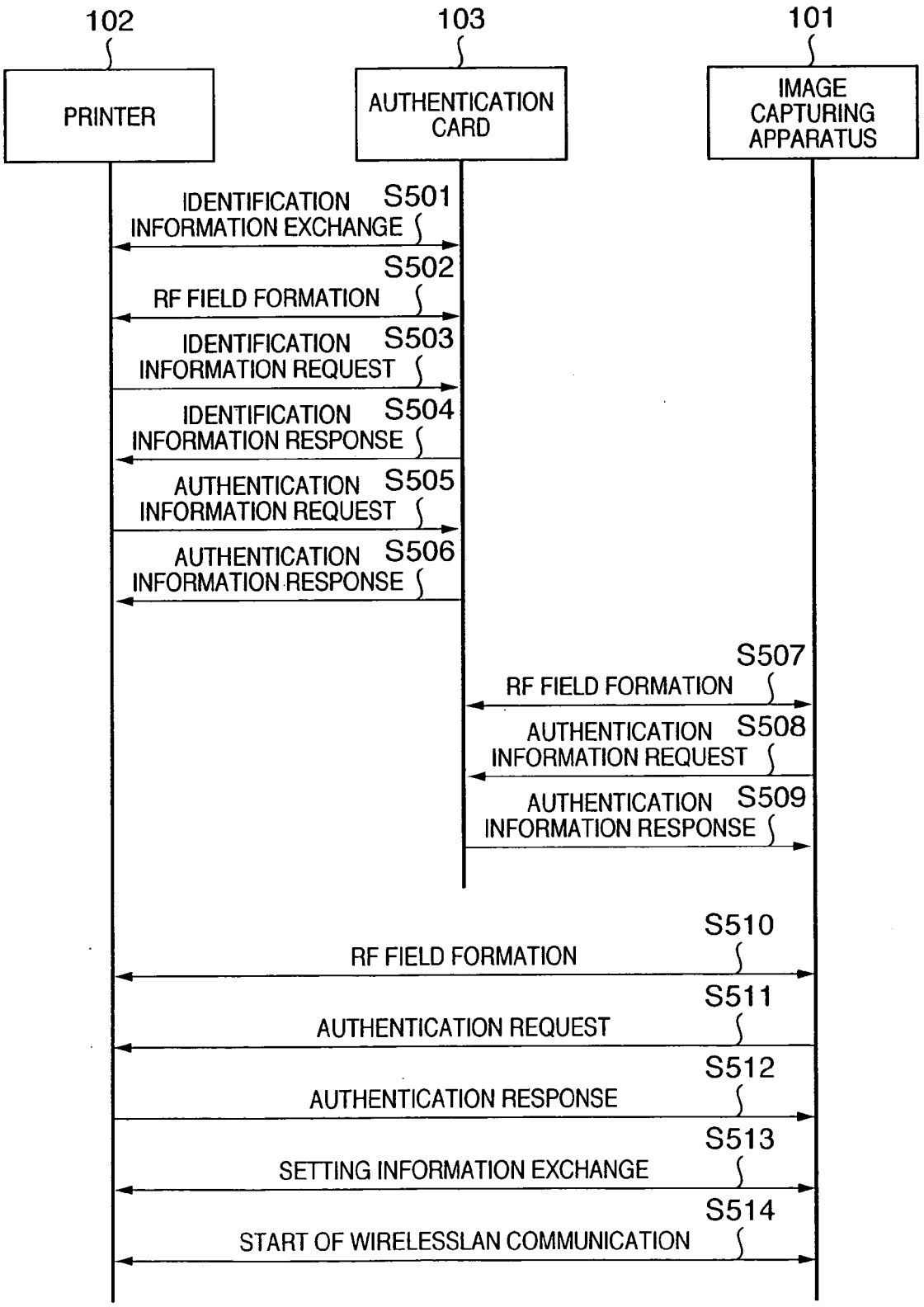

102
103
101
PRINTER
AUTHENTICATION CARD
IMAGE CAPTURING APPARATUS
IDENTIFICATION INFORMATION EXCHANGE
S501
RF FIELD FORMATION
S502
IDENTIFICATION INFORMATION REQUEST
S503
IDENTIFICATION INFORMATION RESPONSE
S504
AUTHENTICATION INFORMATION REQUEST
S505
AUTHENTICATION INFORMATION RESPONSE
S506
RF FIELD FORMATION
S507
AUTHENTICATION INFORMATION REQUEST
S508
AUTHENTICATION INFORMATION RESPONSE
S509
RF FIELD FORMATION
S510
AUTHENTICATION REQUEST
S511
AUTHENTICATION RESPONSE
S512
SETTING INFORMATION EXCHANGE
S513
START OF WIRELESSLAN COMMUNICATION
S514

FIG. 6

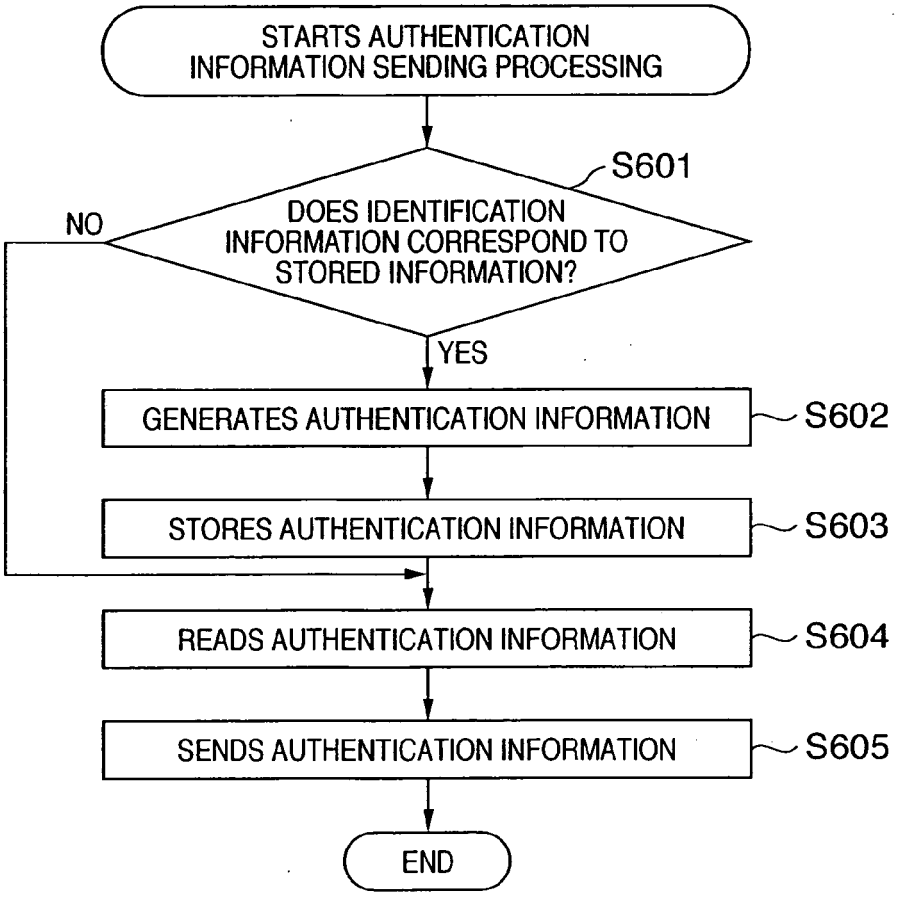

STARTS AUTHENTICATION INFORMATION SENDING PROCESSING
S601
DOES IDENTIFICATION INFORMATION CORRESPOND TO STORED INFORMATION?
NO
YES
GENERATES AUTHENTICATION INFORMATION
S602
STORES AUTHENTICATION INFORMATION
S603
READS AUTHENTICATION INFORMATION
S604
SENDS AUTHENTICATION INFORMATION
S605
END

FIG. 7

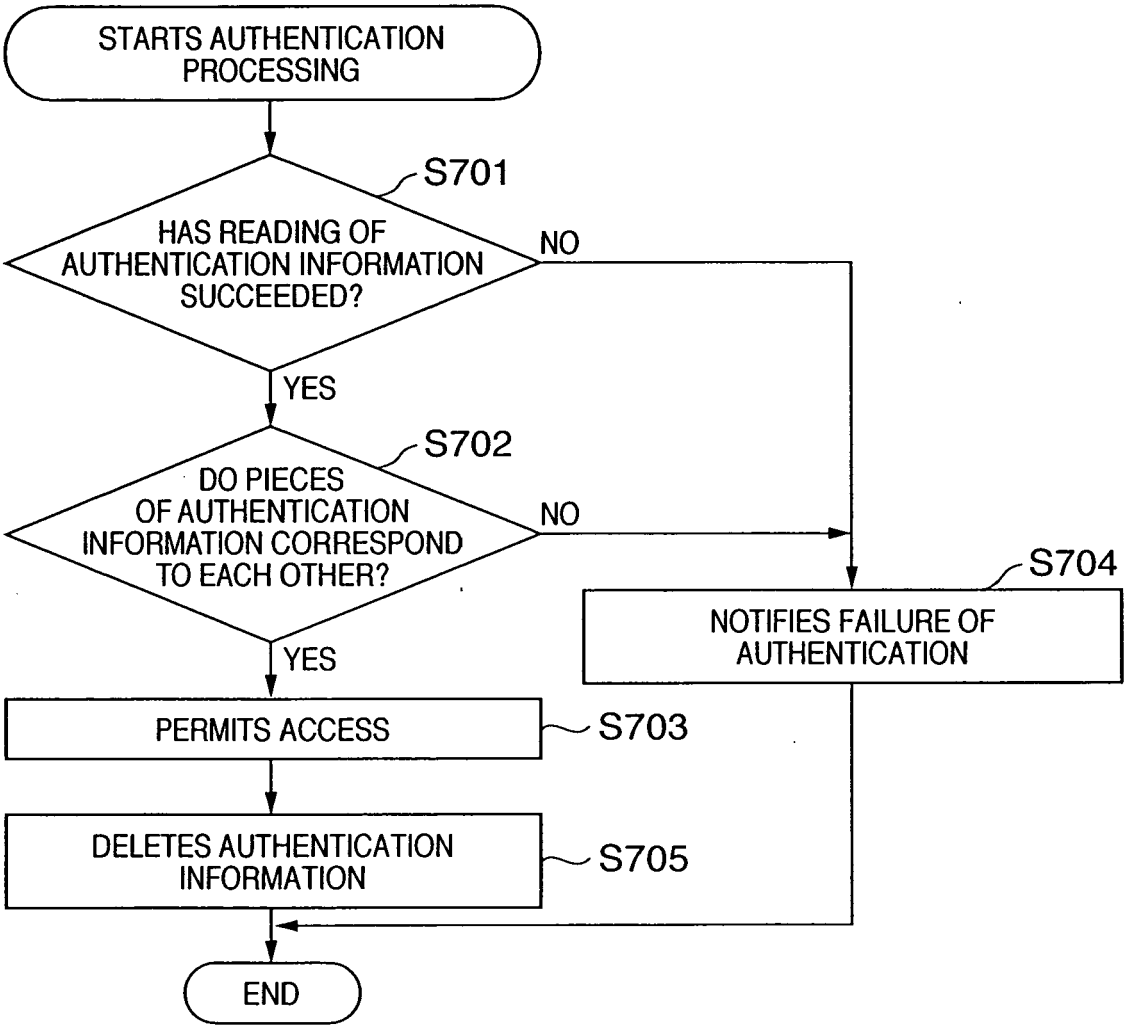

STARTS AUTHENTICATION PROCESSING
S701
HAS READING OF AUTHENTICATION INFORMATION SUCCEEDED?
NO
YES
S702
DO PIECES OF AUTHENTICATION INFORMATION CORRESPOND TO EACH OTHER?
NO
YES
S704
NOTIFIES FAILURE OF AUTHENTICATION
PERMITS ACCESS
S703
DELETES AUTHENTICATION INFORMATION
S705
END

FIG. 8

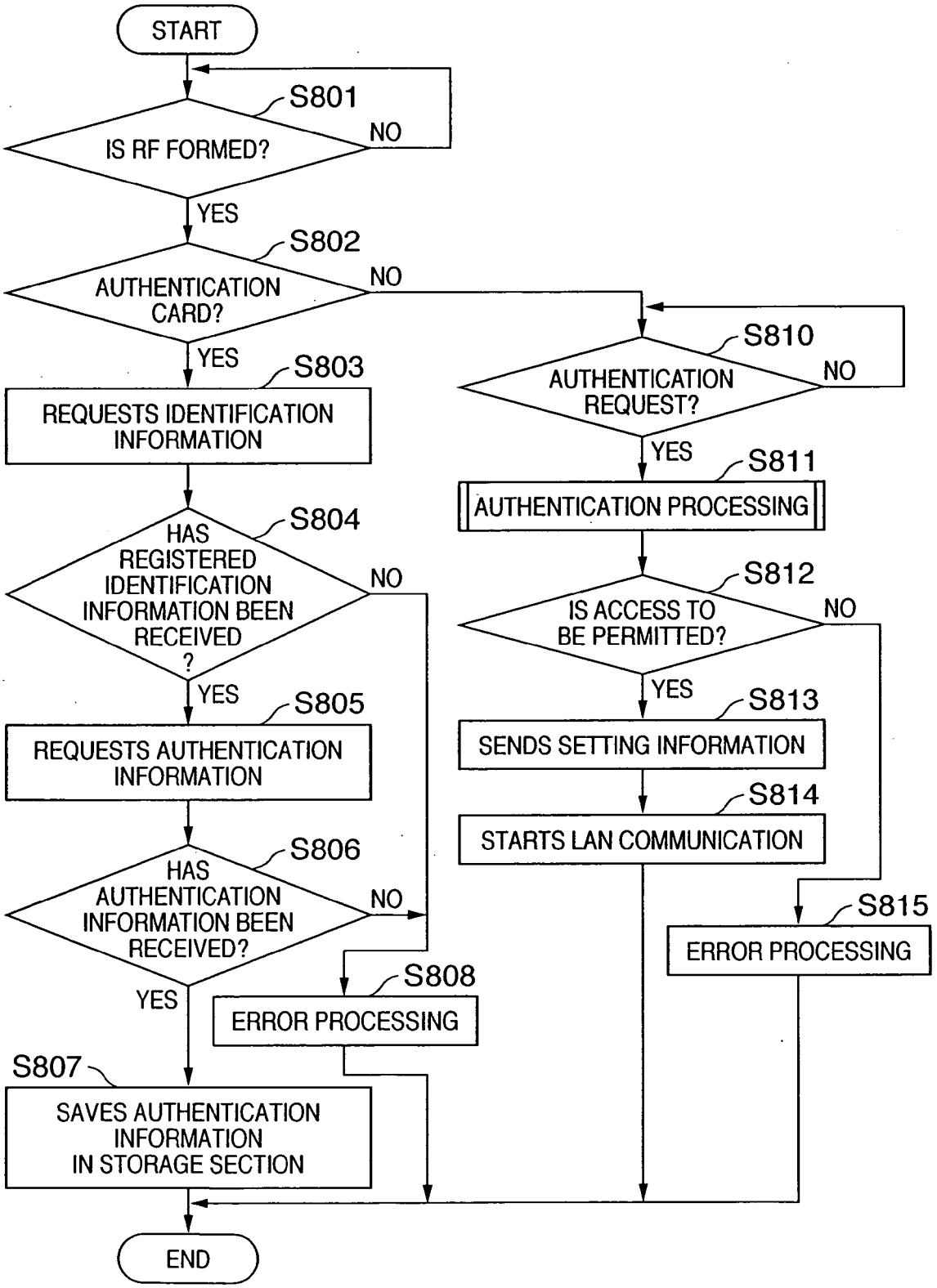

START
S801
IS RF FORMED?
NO
YES
S802
AUTHENTICATION CARD?
NO
YES
S803
REQUESTS IDENTIFICATION INFORMATION
S804
HAS REGISTERED IDENTIFICATION INFORMATION BEEN RECEIVED ?
NO
YES
S805
REQUESTS AUTHENTICATION INFORMATION
S806
HAS AUTHENTICATION INFORMATION BEEN RECEIVED?
NO
YES
S807
SAVES AUTHENTICATION INFORMATION IN STORAGE SECTION
S808
ERROR PROCESSING
END
S810
AUTHENTICATION REQUEST?
NO
YES
S811
AUTHENTICATION PROCESSING
S812
IS ACCESS TO BE PERMITTED?
NO
YES
S813
SENDS SETTING INFORMATION
S814
STARTS LAN COMMUNICATION
S815
ERROR PROCESSING

FIG. 9

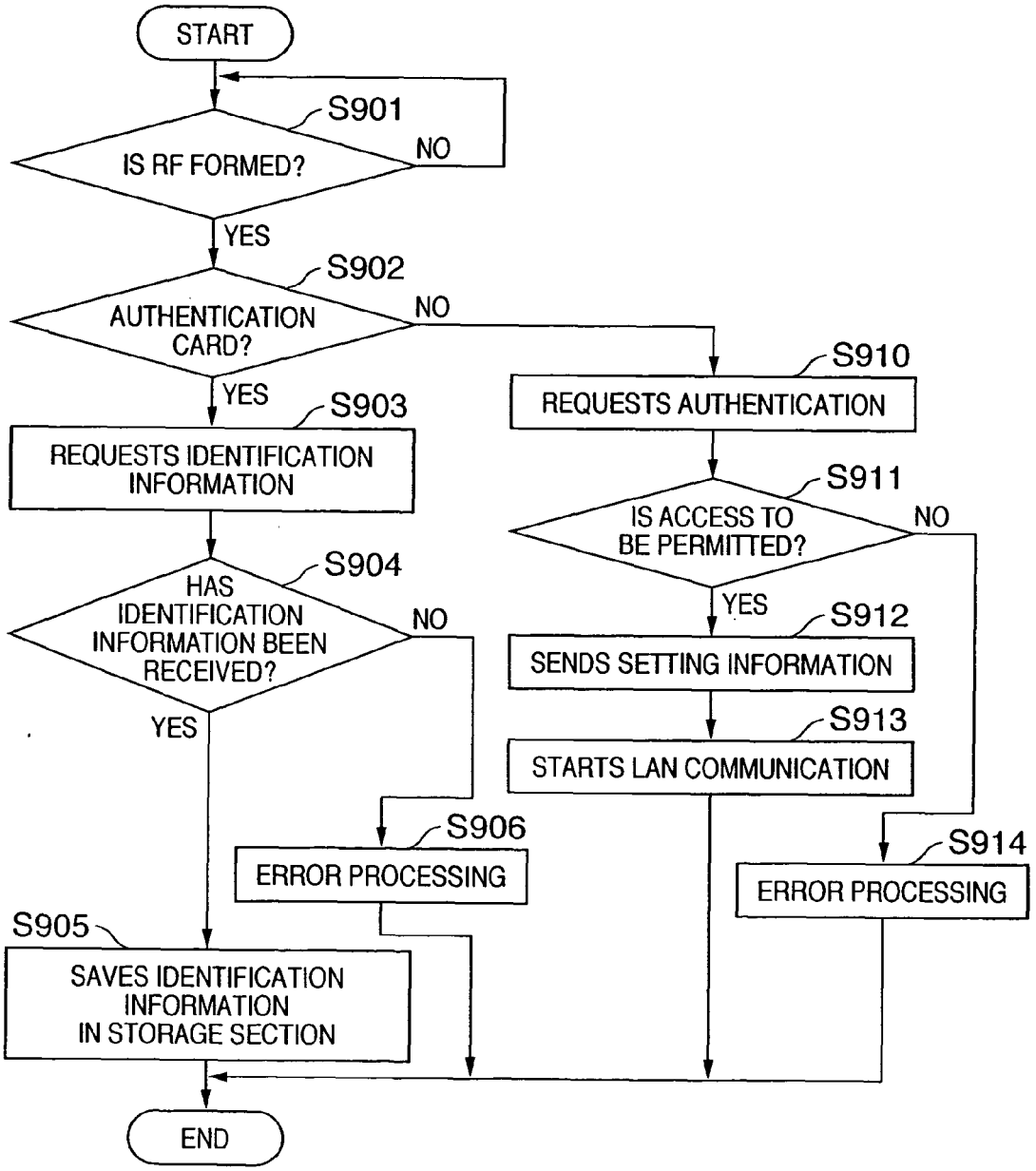
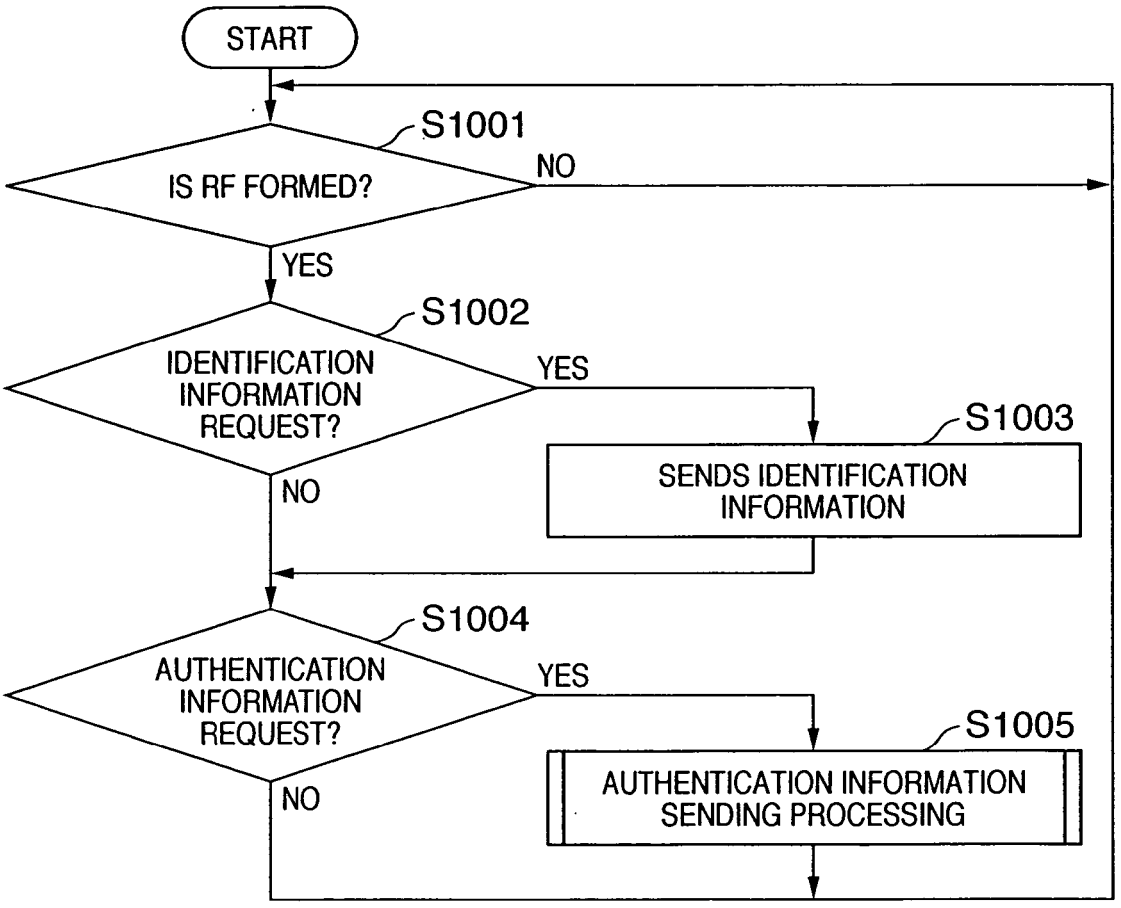

START
S901
IS RF FORMED?
NO
YES
S902
AUTHENTICATION CARD?
NO
YES
S903
REQUESTS IDENTIFICATION INFORMATION
S904
HAS IDENTIFICATION INFORMATION BEEN RECEIVED?
NO
YES
S905
SAVES IDENTIFICATION INFORMATION IN STORAGE SECTION
S906
ERROR PROCESSING
S910
REQUESTS AUTHENTICATION
S911
IS ACCESS TO BE PERMITTED?
NO
YES
S912
SENDS SETTING INFORMATION
S913
STARTS LAN COMMUNICATION
S914
ERROR PROCESSING
END

FIG. 10


START
S1001
IS RF FORMED?
NO
YES
S1002
IDENTIFICATION INFORMATION REQUEST?
YES
S1003
SENDS IDENTIFICATION INFORMATION
NO
S1004
AUTHENTICATION INFORMATION REQUEST?
YES
S1005
AUTHENTICATION INFORMATION SENDING PROCESSING
NO

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 02 3076

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	PATENT ABSTRACTS OF JAPAN vol. 2000, no. 24, 11 May 2001 (2001-05-11) & JP 2001 189722 A (TOSHIBA CORP), 10 July 2001 (2001-07-10) * abstract * -----	1-17	H04L29/06 H04L12/28 G06F1/00 G06K19/00
X	PATENT ABSTRACTS OF JAPAN vol. 2003, no. 10, 8 October 2003 (2003-10-08) & JP 2003 174468 A (SONY CORP), 20 June 2003 (2003-06-20) * abstract * -----	1-17	
X	EP 1 437 863 A (SONY CORPORATION) 14 July 2004 (2004-07-14) * abstract * * paragraph [0019] - paragraph [0049] * * paragraph [0052] - paragraph [0053] * * paragraph [0057] - paragraph [0061] * * paragraph [0122] - paragraph [0123] * * paragraph [0187] * * figures 1,2,5,16,17,19 * -----	1-17	TECHNICAL FIELDS SEARCHED (IPC) H04L G06F G06K
A	EP 1 182 825 A (KABUSHIKI KAISHA TOSHIBA) 27 February 2002 (2002-02-27) * abstract * * paragraph [0010] - paragraph [0011] * -----	1-17	
A	EP 1 335 563 A (XEROX CORPORATION) 13 August 2003 (2003-08-13) * abstract * * paragraph [0003] - paragraph [0013] * * paragraph [0015] - paragraph [0022] * * paragraph [0025] * * paragraph [0029] * * paragraph [0031] * ----- -/--	1-17	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	13 February 2006	Kopp, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 02 3076

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 02/03625 A (PHILLIPPS, JOHN, QUENTIN) 10 January 2002 (2002-01-10) * abstract * * page 1, line 21 - page 3, line 2 * * page 4, line 4 - line 10 * * page 5, line 1 - page 9, line 2 * * page 9, line 31 - page 10, line 2 * -----	1-17	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	13 February 2006	Kopp, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
.....
& : member of the same patent family, corresponding document

1 EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 02 3076

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

13-02-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2001189722 A	10-07-2001	NONE	
JP 2003174468 A	20-06-2003	JP 3687599 B2	24-08-2005
		US 2003110512 A1	12-06-2003
EP 1437863 A	14-07-2004	CN 1572087 A	26-01-2005
		WO 03034660 A1	24-04-2003
		US 2004242250 A1	02-12-2004
EP 1182825 A	27-02-2002	JP 2002140304 A	17-05-2002
		US 2002025042 A1	28-02-2002
EP 1335563 A	13-08-2003	JP 2003309558 A	31-10-2003
		US 2003149874 A1	07-08-2003
WO 0203625 A	10-01-2002	AU 5238401 A	14-01-2002
		BR 0112087 A	06-05-2003
		CA 2414845 A1	10-01-2002
		CN 1439214 A	27-08-2003
		EP 1297658 A1	02-04-2003
		GB 2364457 A	23-01-2002
		JP 2004503138 T	29-01-2004
		US 2004203376 A1	14-10-2004

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82